TEMPEST

ATAQUES & DEFESAS

Diego Protta Casati

(kzaty)

Network Security, Internet Security, Information Technology Security Fundamentals, ITAA Information Security Awareness Brainbench Certified

NextGeneration - Segurança

Esta obra está licenciada sob uma Licença Creative Commons

http://creativecommons.org

Verdadeiro ou Falso?

"Agência de segurança descobre técni[illegible] interceptação e captura de ondas eletromagnéticas [illegible] monitor a centenas de metros d[illegible]ia. "

VERDADE

"Pesquisador quebra proteçã[illegible]tcard apenas monitorando as variações [illegible] de alimentação."

VERDADE

"Monitores de LCD sã[illegible]munes a vazamentos ele[illegible]néticos."

MENTIRA

Quem sou eu?

- Software Livre: OpenBSD,
- Linux (Slackware, Red Hat)

- Lucent Global Scholar
- Suporte Técnico - Inatel
- SandStorm – InfoSec
- Primeiro Encontro de Software Livre na UFES - 2004

O que significa Tempest?

TEMPEST

" ...é código do governo dos EUA para uma série de padrões com o objetivo em limitar a irradiação elétrica ou eletromagnética de equipamentos eletrônicos como microchips, monitores, ou impressoras. É um medida de contra-inteligência apontada para a prevenção de espionagem eletrônica. (EMSEC – Emission Security)"

http://en.wikipedia.org/wiki/Emission_security

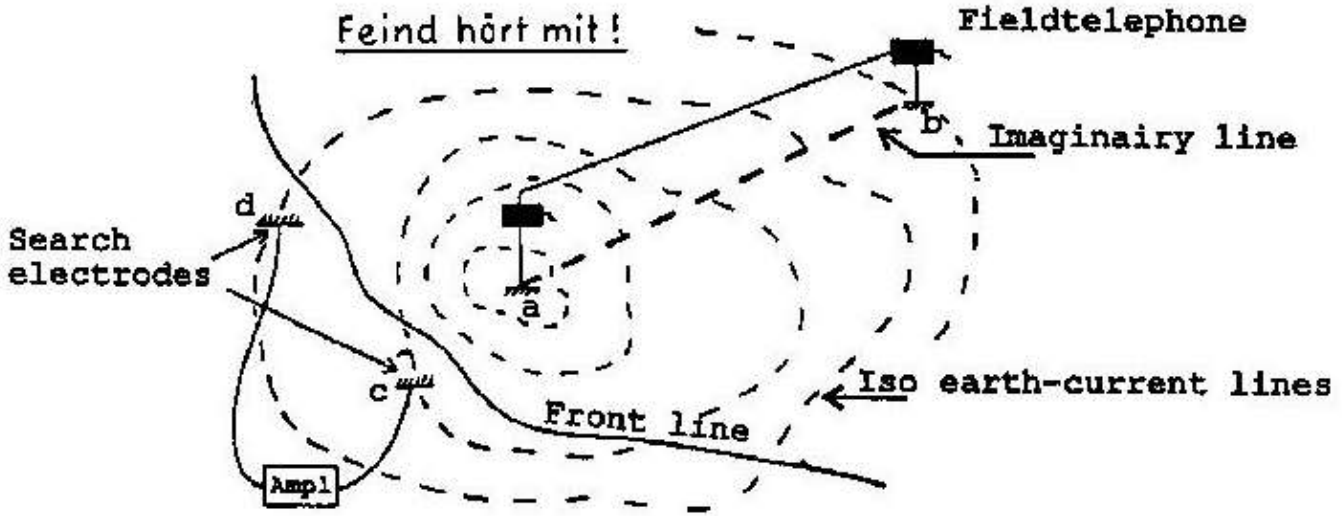
Quem está a salvo?

- Praticamente NINGUÉM!!!!!

Dispositivos eletrônicos como:

- Impressoras
- Monitores com CRT (Tubos de Raios Catódicos)
- Teclados
- Mouses
- Monitores de LCD!!!!!!
- HDs

Histórico



The German army started in 1914 to use valve amplifiers for listening into ground return signals of distant British, French and Russian field telephones across front lines [Bauer, 1999].

Normas, documentos e informações

· Poucas informações públicas.
· Algumas referências no final da apresentação
· Google ! :-D

· NSTISSAM TEMPEST1-92 (Freedom-of-Information-Act)
· NACSIM 5000: Tempest Fundamentals
· AMSG 720B (OTAN)

Limites de emanação, testes, procedimentos e inclusive alguns termos permanecem como segredos militares.

Princípios do Eletromagnetismo?

A aceleração de cargas elétricas resulta na geração de um campo eletromagnético variável.

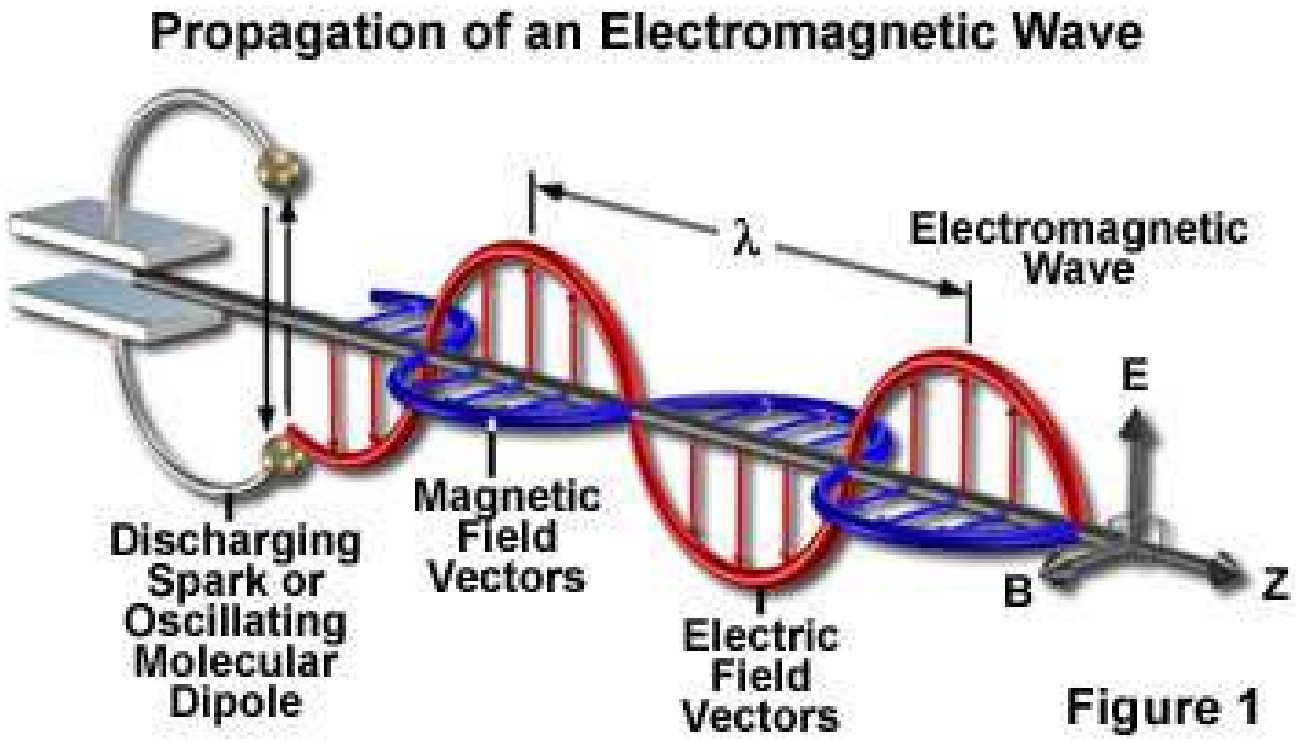
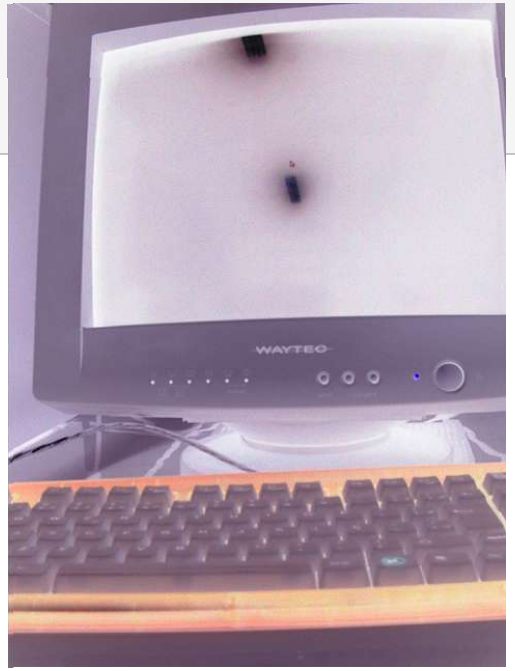


Figure 1

Como?

· Operação normal do sistema
· Exposição acidental ou deliberada de um sistema a um ambiente atípico
· Execução de um software com o propósito de modular dados em energia



O Fenômeno

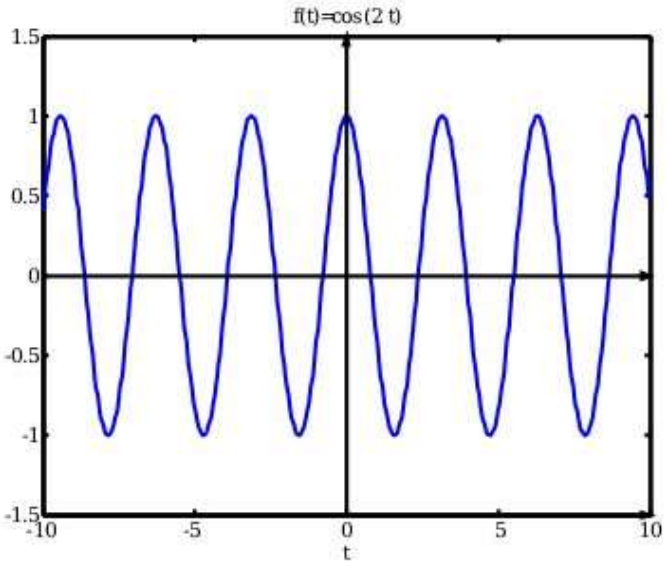
Aplicação de sinais de onda quadrada em altas frequências nos equipamentos digitais leva a irradiação de campos eletromagnéticos contendo componentes até a faixa de UHF. (300 – 3000 MGHz)

Inútil contra ataques Tempest

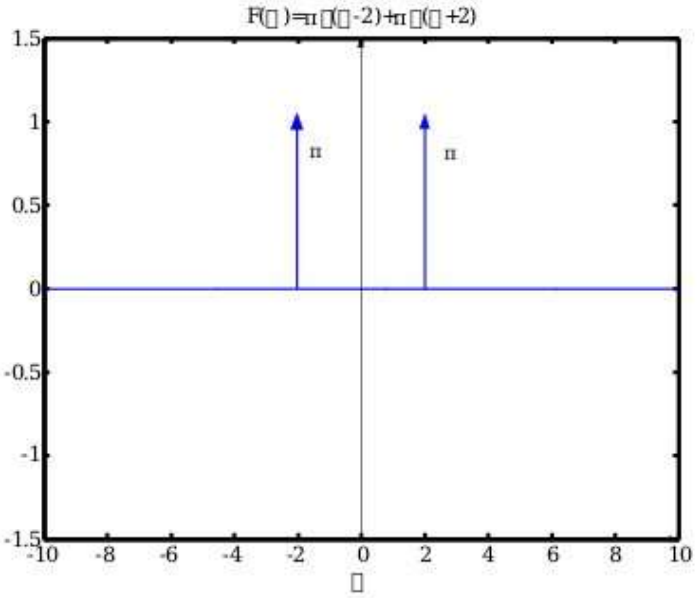
- Criptografia
- Segurança Física (Biometria, Íris, Digitais)
- Controle de Acesso via software (ACL)
- Firewalls
- Proteções na Pilha, memória, etc.
- Segurança no Sistema Operacional
- Bulldogs, pitbulls, yoda, McGuiver.... :-D

Domínio do Tempo vs Frequência

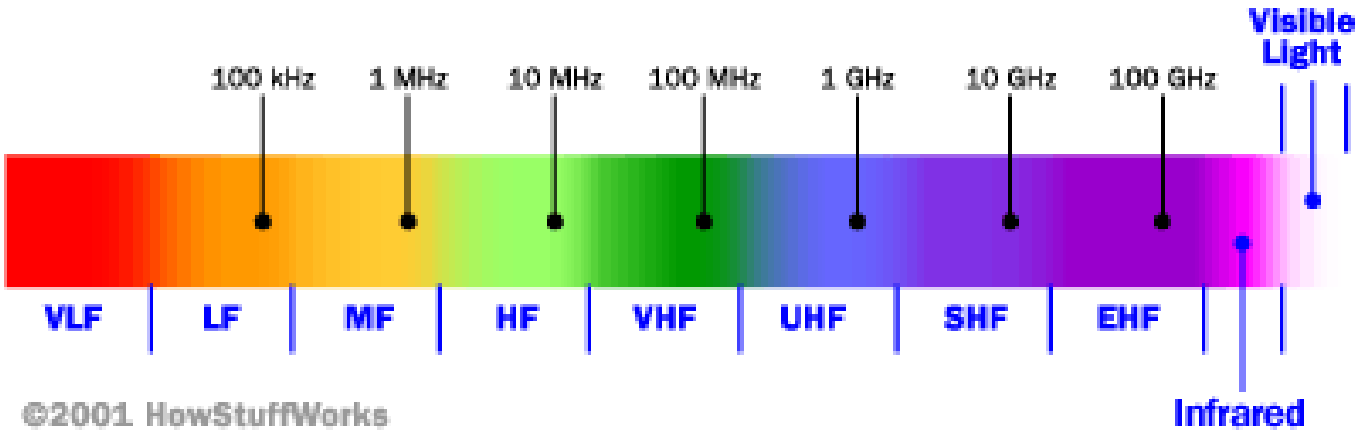
Osciloscópio



Analisador de Espectro

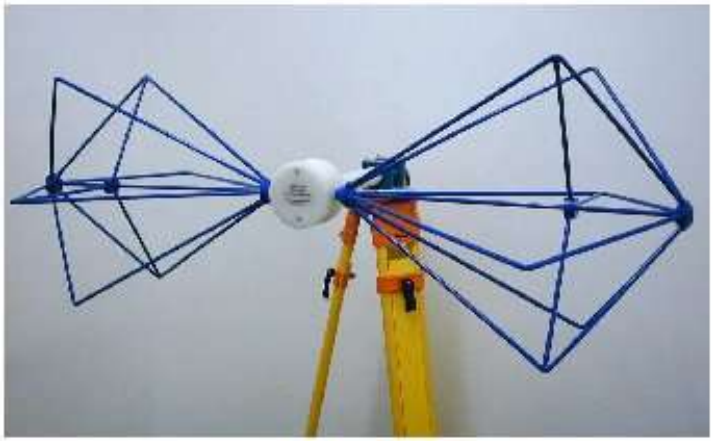


Propagação Eletromagnética

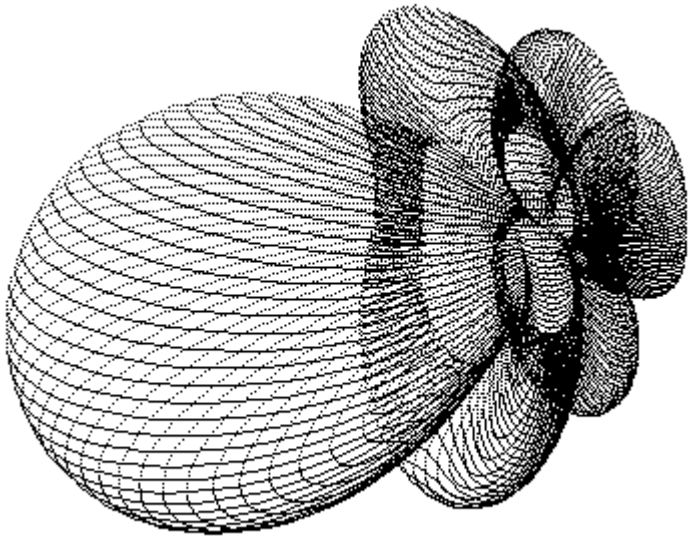


VF	Voice Frequencies	Frequências de voz
LF	Low Frequencies	Ondas Longas
MF	Medium Frequencies	Ondas Médias
HF	**High Frequencies**	**Ondas Curtas**
VHF	Very High Frequencies	Onda Muito Curtas
UHF	Ultra High Frequencies	Microondas
SHF	Super High Frequencies	Microondas
EHF	Extremely High Frequencies	Microondas

Antenas



Yagi-uda

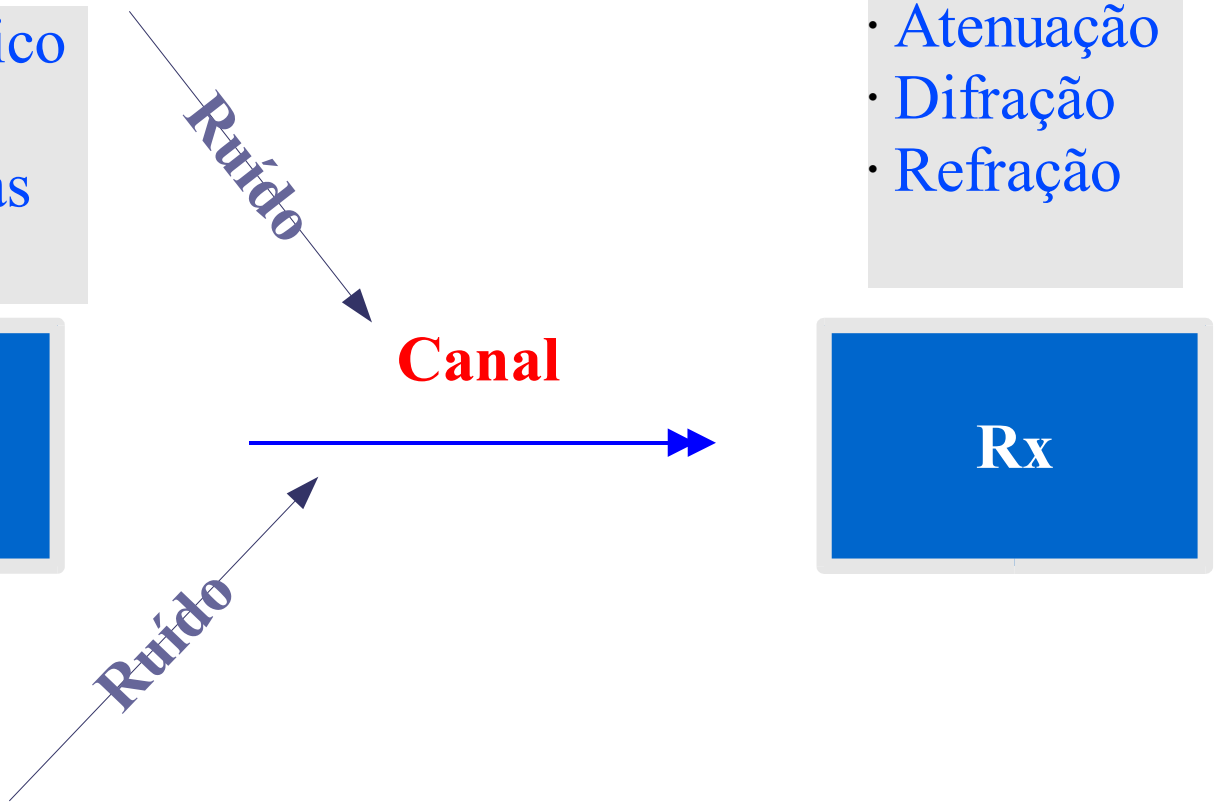


JM1SZY WIDEBANDWIDTH 9-ELEMENT YAGI

- Fácil contrução.
- 50 MHz a 1GHz.
- Ganho Ajustável
- Diretividade
- Fácil ocultação

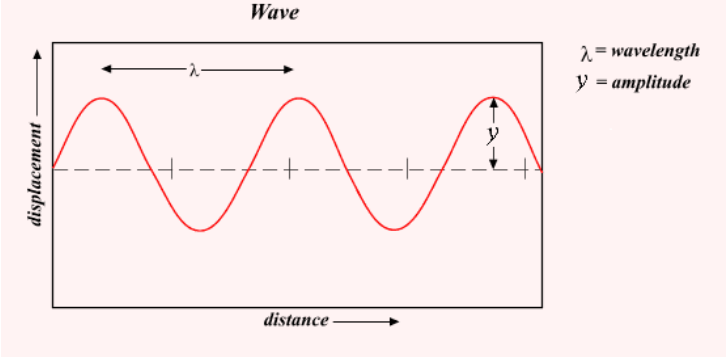
Princípios das Comunicações

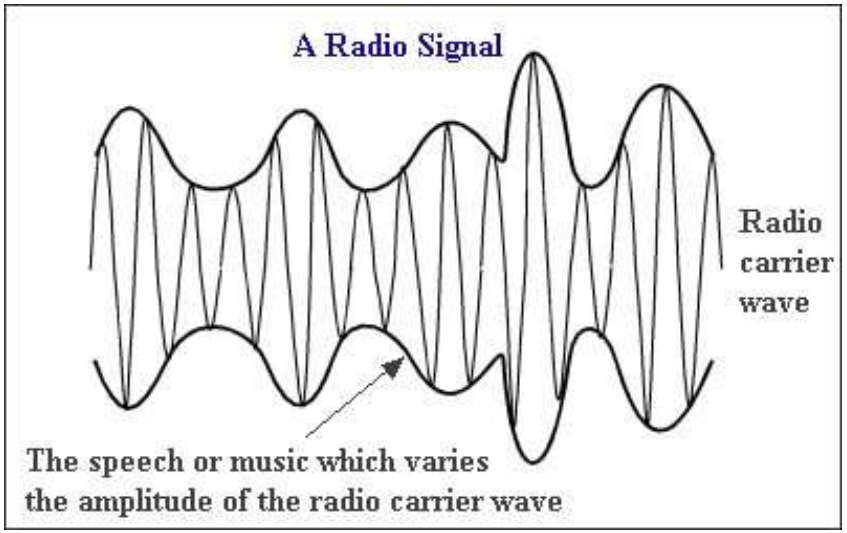
- Ruído Térmico
- Quantização
- Interferências



- Atenuação
- Difração
- Refração

Princípios das Comunicações II





Informação
Baixa Frequência

Portadora
Alta Frequência

Os Ataques

Optical Tempest

Diretamente – Com uma luneta é possível observar um monitor com a resolução de 1280x1024 a 60 m de distância

Teorema de Rayleigh

$$D = (1.22 \lambda d) / r \cos$$

Onde:

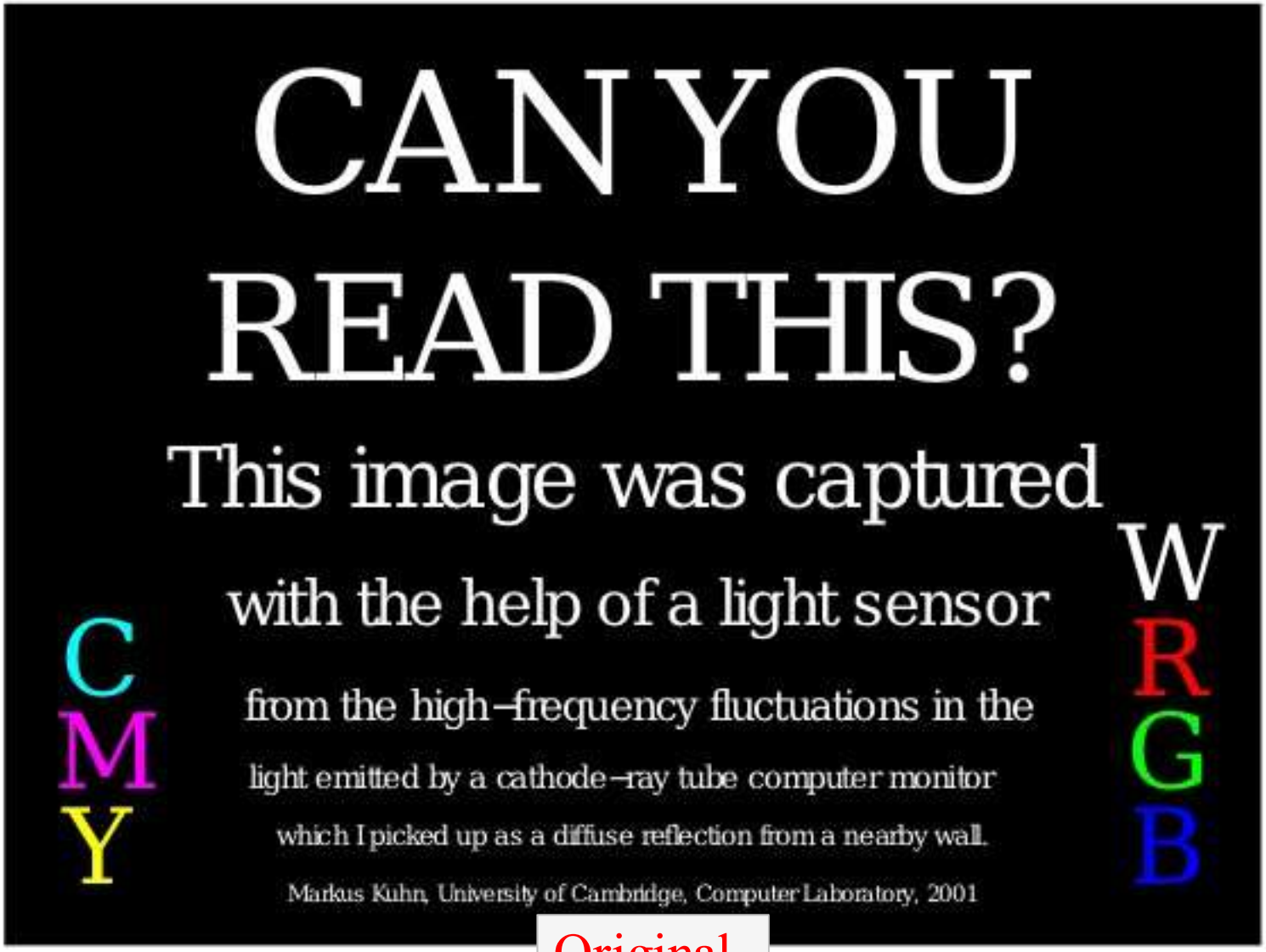
Lambda = 500 nm
r = .25 mm (tamanho de um pixel)
Display de 320 x 240 mm
CRT de aprox. 43 cm

Optical Tempest

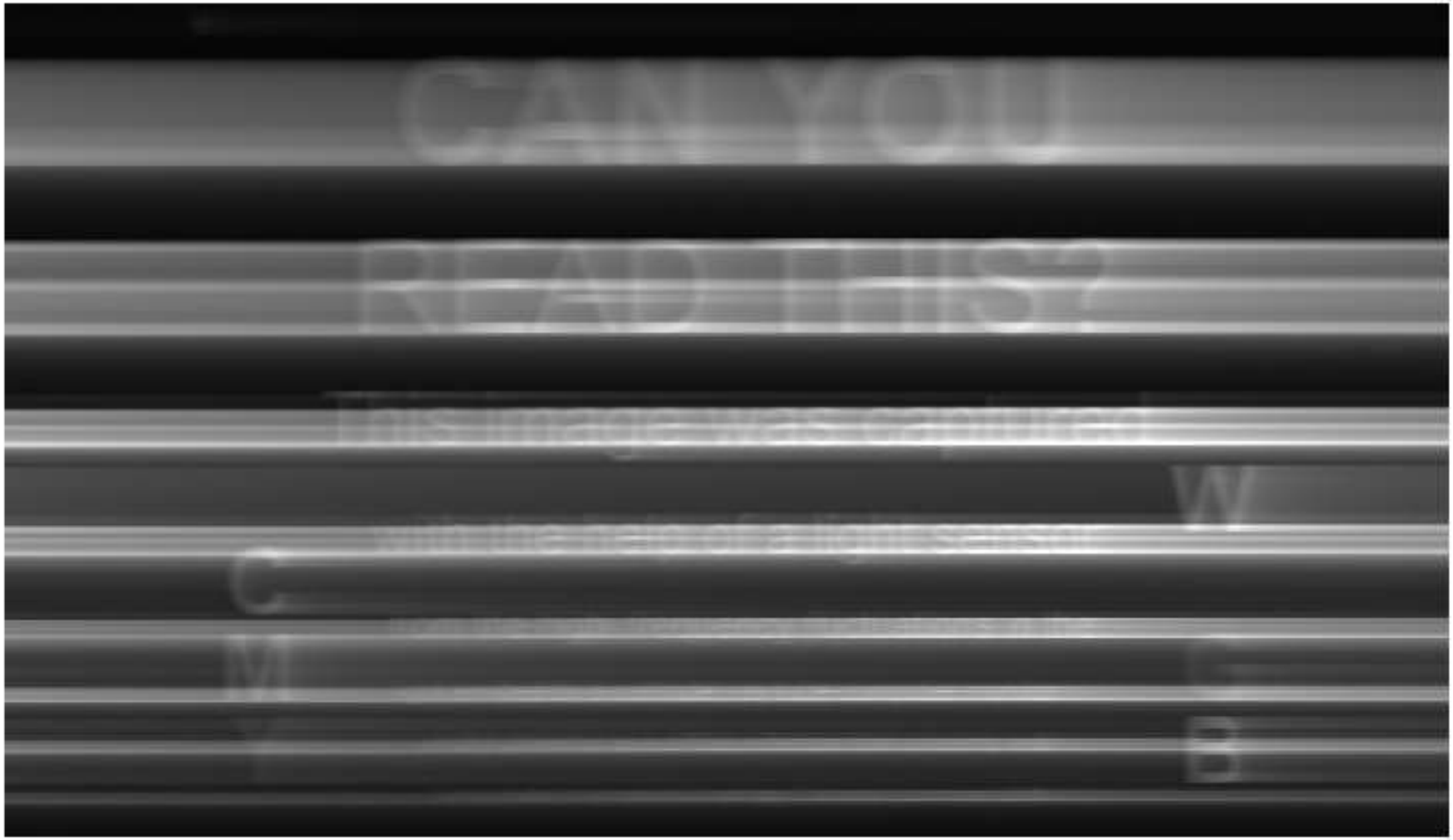
Indiretamente – Variações de amplitudes em sinais de alta frequências no CRT dependem no sinal de vídeo.

Persianas, cortinas, vidro fumê não conseguem bloquear 100% dessas variações

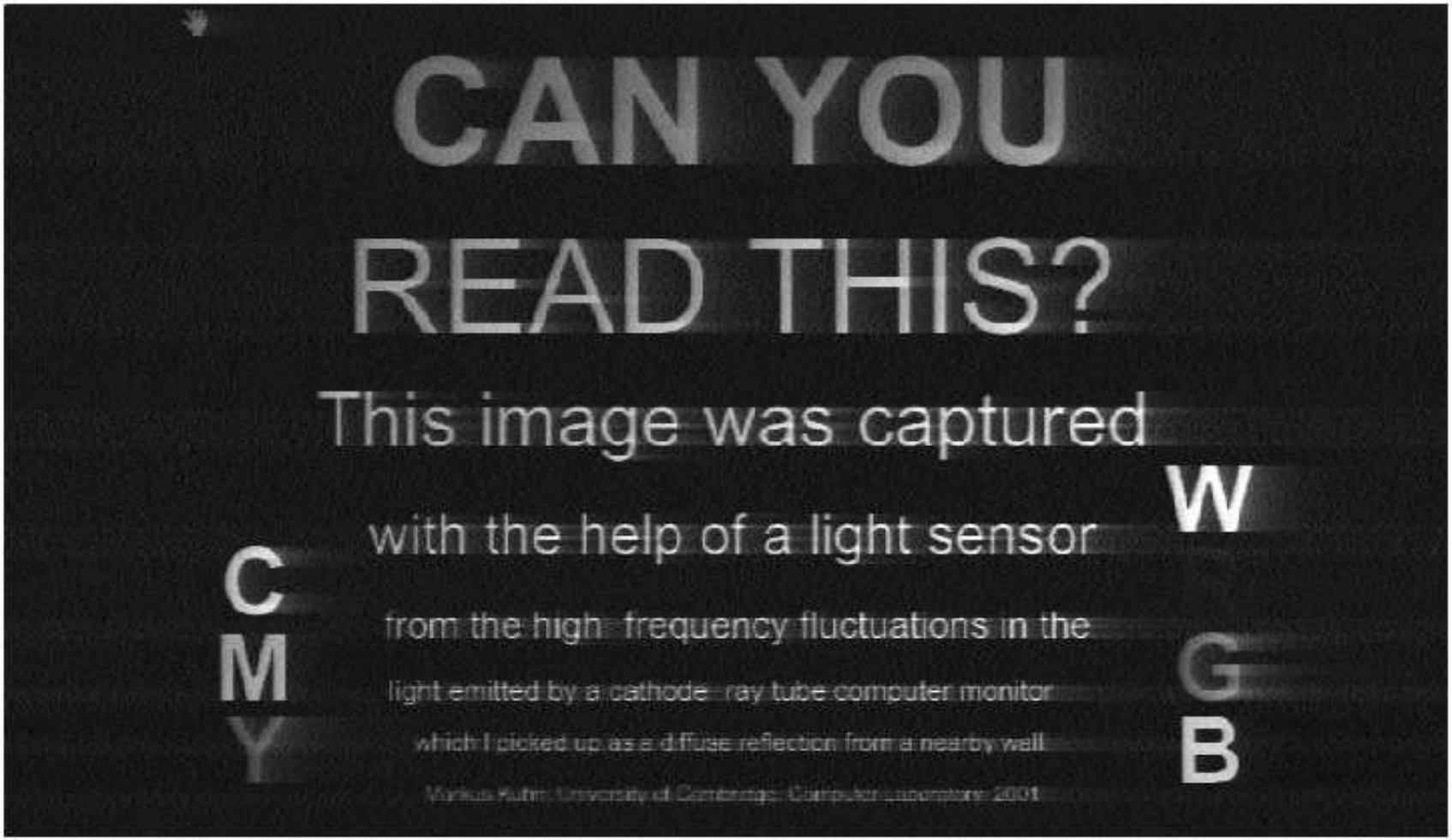
Hamamatsu H6780-01


CAN YOU
READ THIS?
This image was captured
with the help of a light sensor
from the high-frequency fluctuations in the
light emitted by a cathode-ray tube computer monitor
which I picked up as a diffuse reflection from a nearby wall.
Markus Kuhn, University of Cambridge, Computer Laboratory, 2001
C
M
Y
W
R
G
B

Original

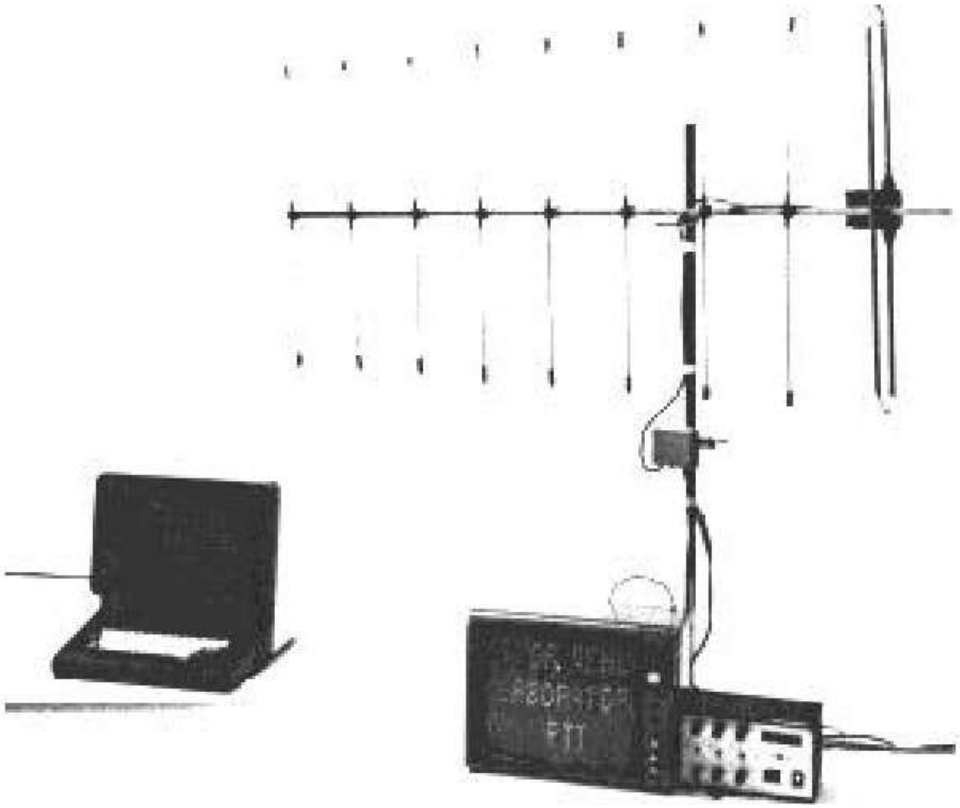


1,5 metros de distância sem filtro



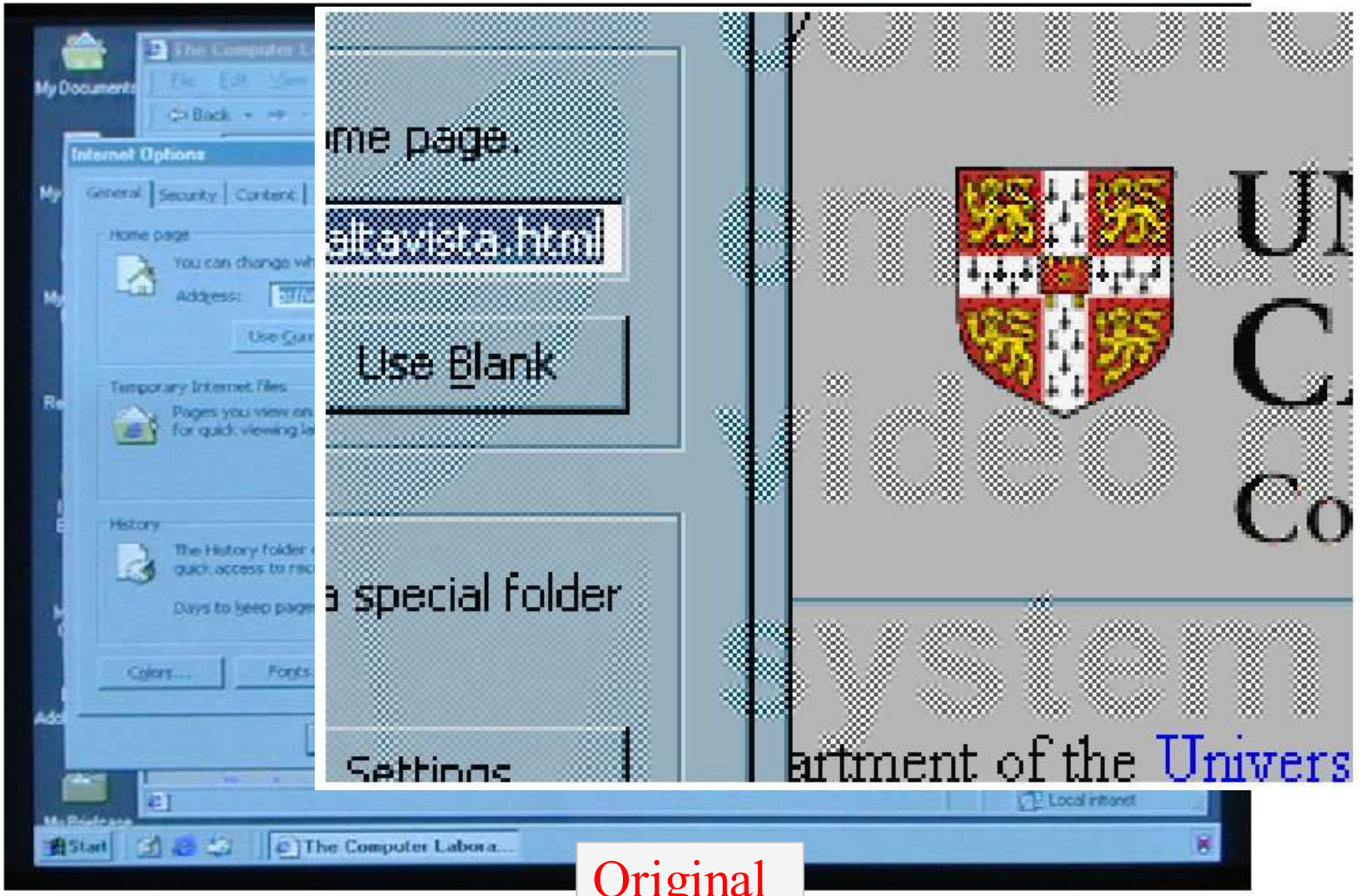
Utilizando filtro casado

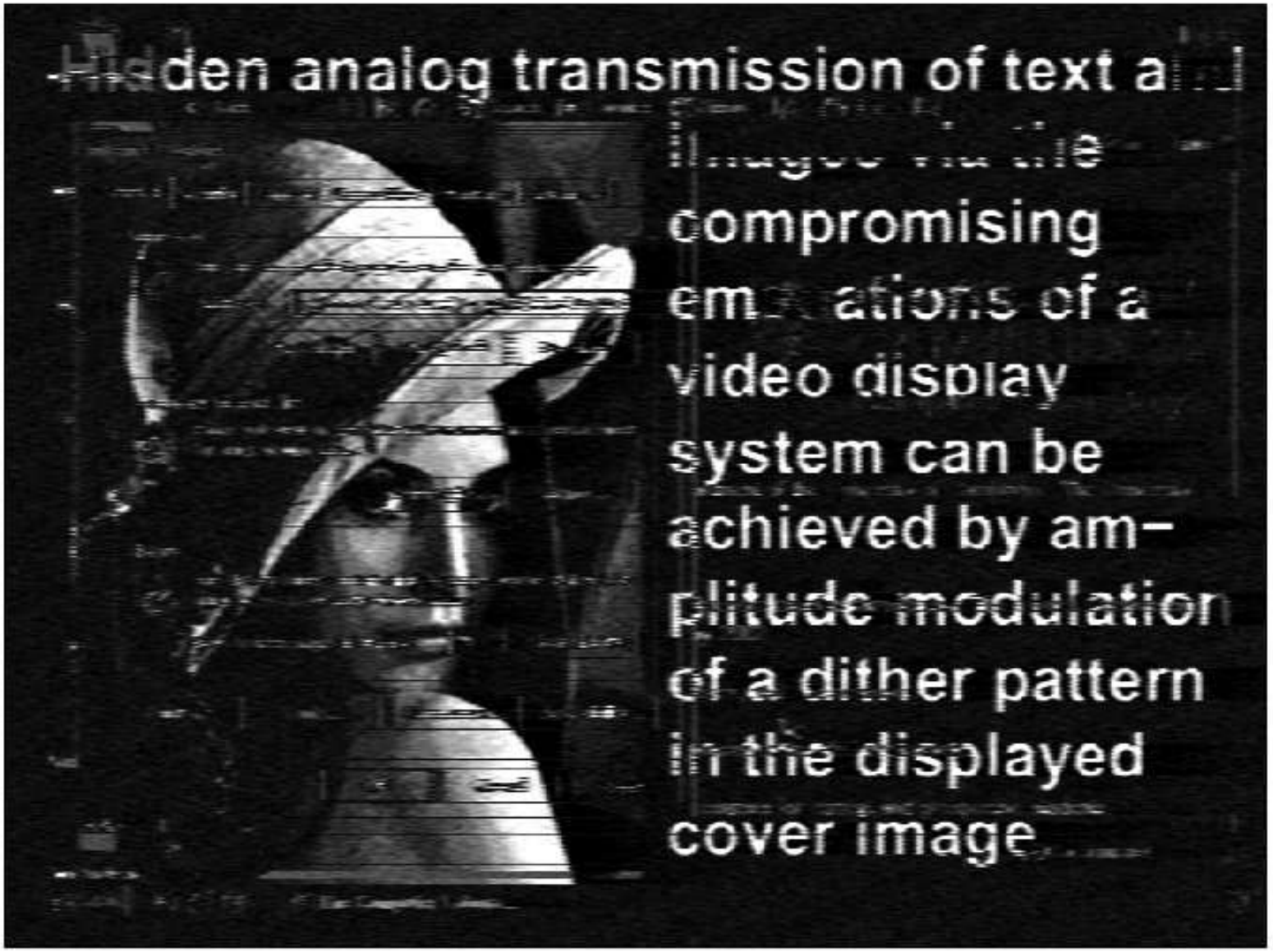
a la “van Eck”



Em alguns casos a ressonância pode aumentar o nível de irradiação para algumas frequências no espectro.

Ofuscação de Dados




Hidden analog transmission of text and
compromising
emanations of a
video display
system can be
achieved by am-
plitude modulation
of a dither pattern
in the displayed
cover image.
9
8
7
6
5
4
3
μV

Nossa aproximação

Rx

Hospedeiro

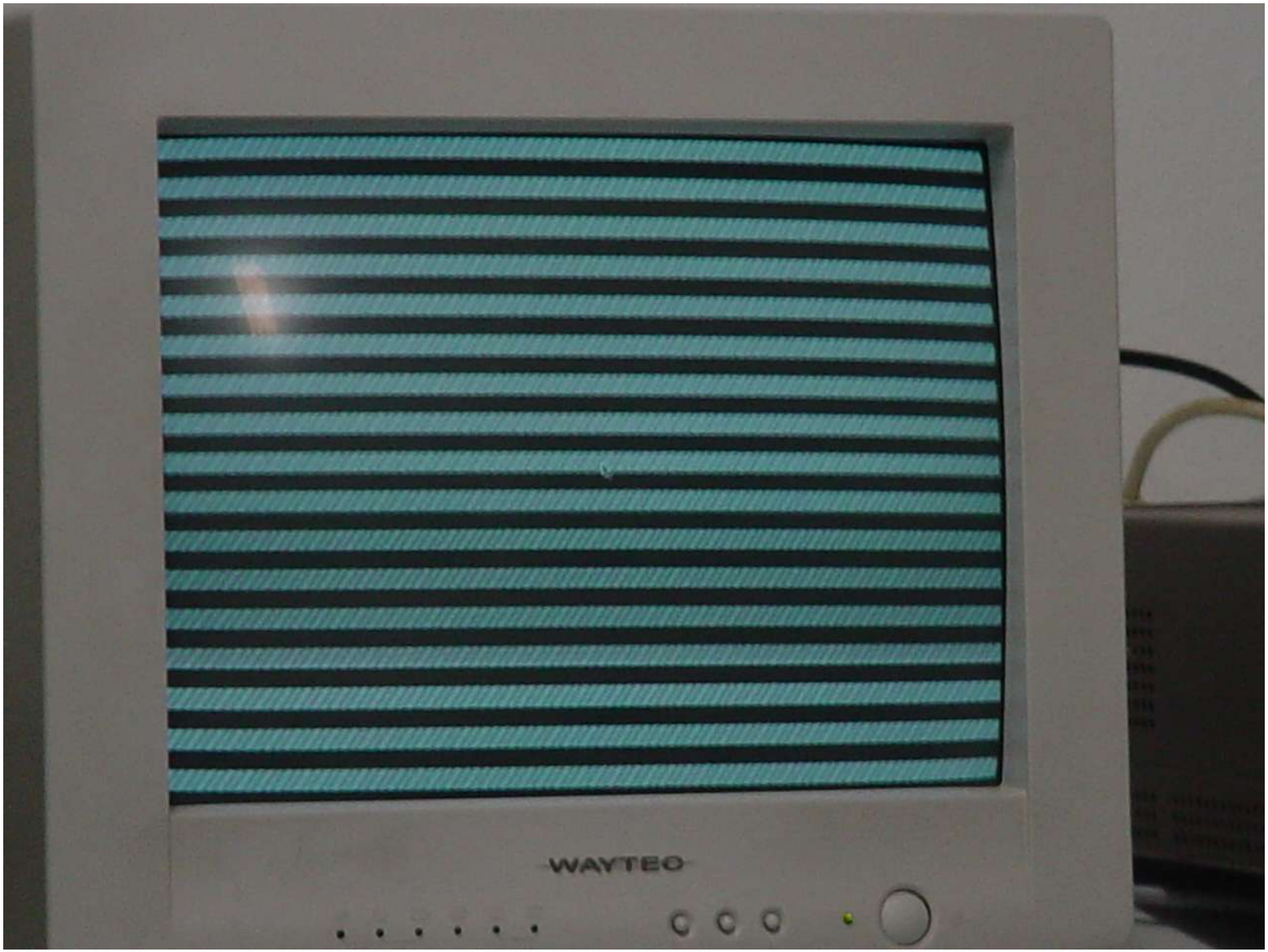
Keylogger

cat /etc/shadow | grep root

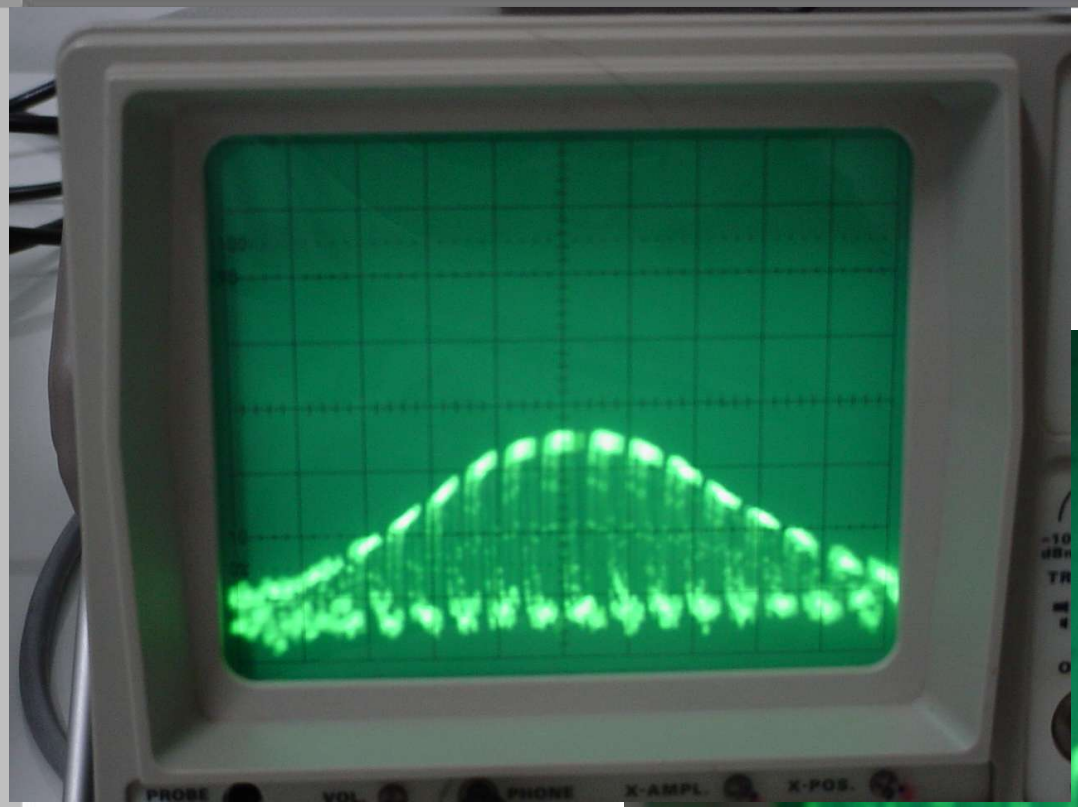
Atacante

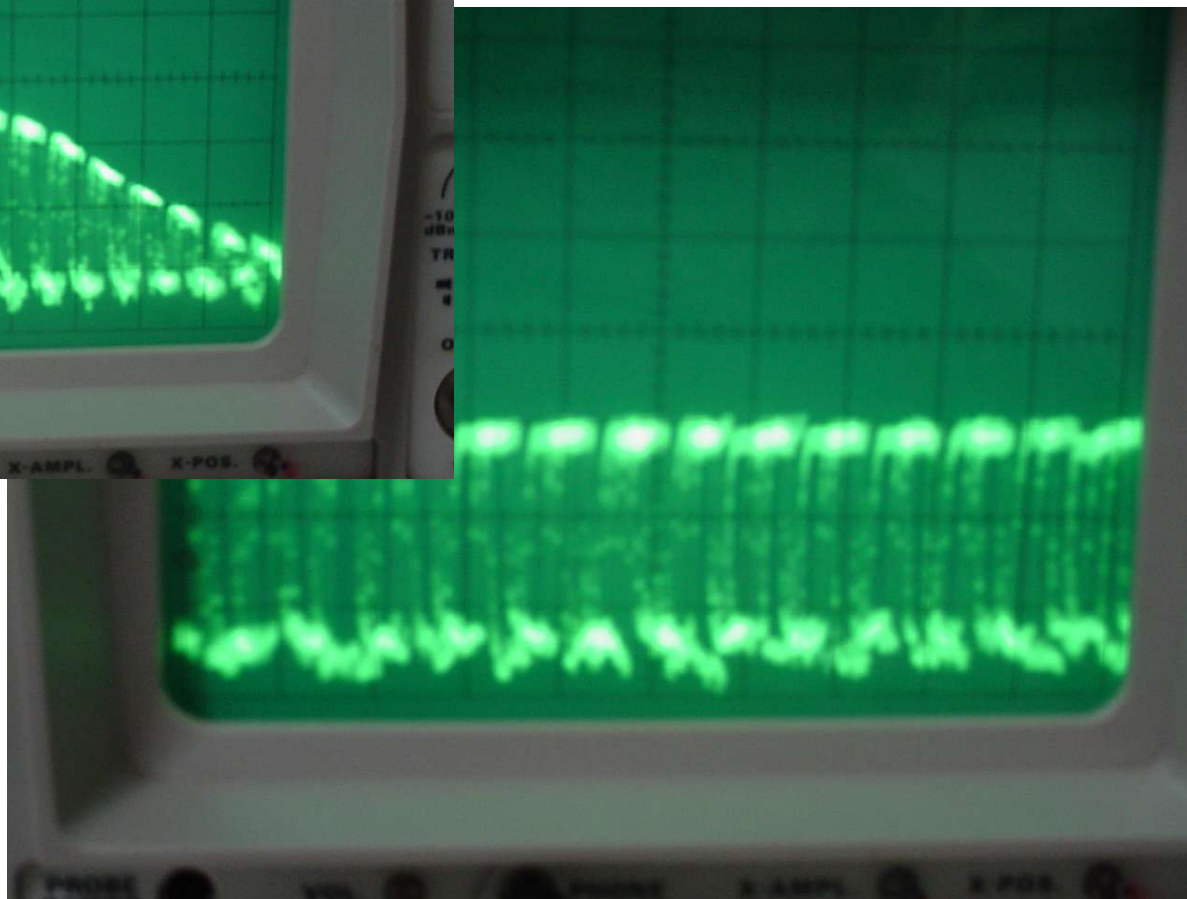
Experiência

- Teste do software “Tempest_for_eliza”
- Analisador de Espectros: Hameg 5011
- Rádio PX – 40 Canais – Faixa do Cidadão: Allan
- Monitor Waytech
- Athlon XP 2000+, 256 MB
- GeForce MX 420 – 64 MB


WAYTEC

TEMPEST
ATAQUES & DEFESAS





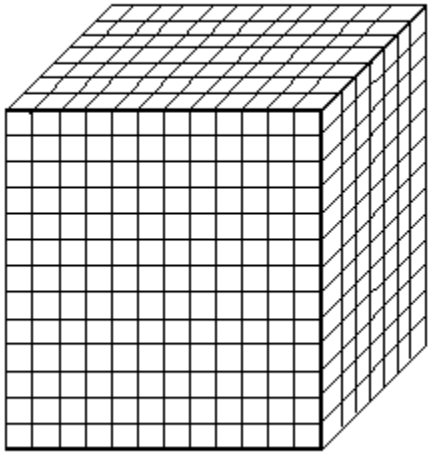
Técnicas de Ataques

Atacantes podem utilizar:

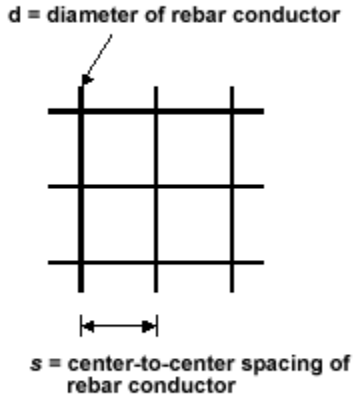
· Antenas de alto ganho e diretividade
· Utilizar filtros para suprimir interferencias de outros sinais
· DSP – Correlação-cruzada, máxima verssimilhança, modulação/demodulação digital, média periódica, convolução.

As Defesas

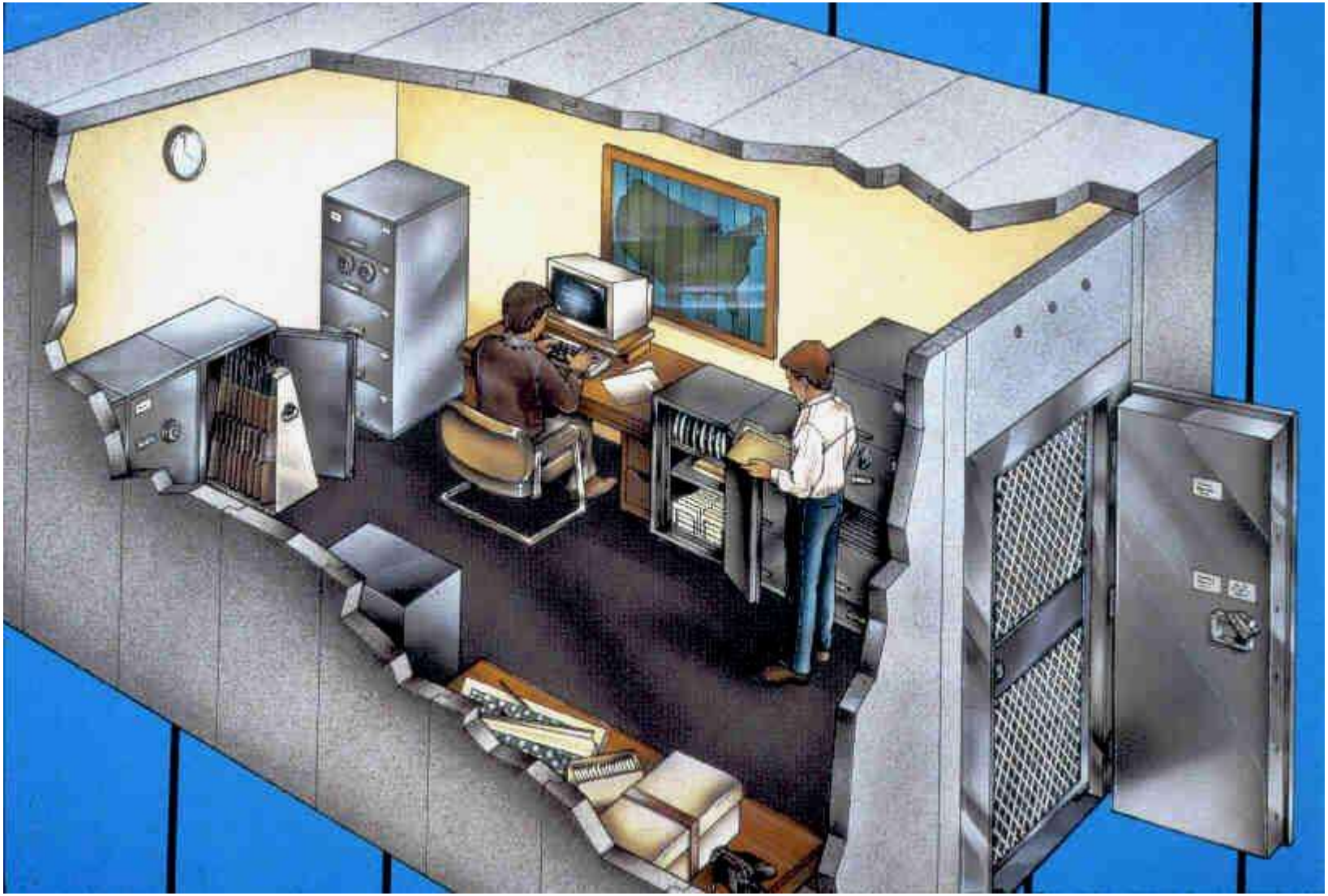
Gaiola de Faraday



Elemental Faraday Cage



TEMPEST
ATAQUES & DEFESAS

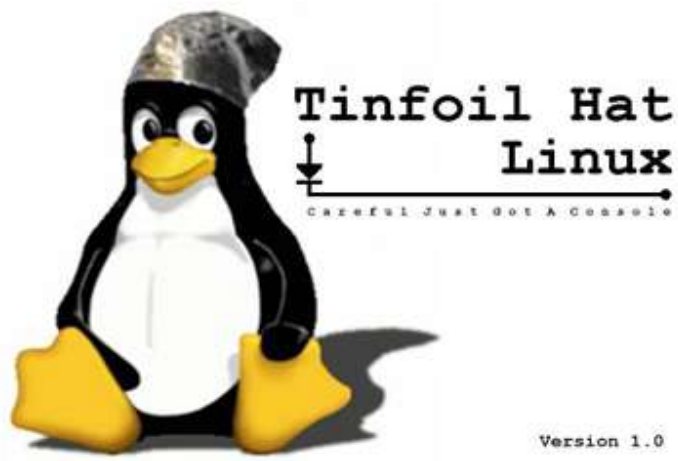


http://www.bemashield.com

Outras alternativas

- Fontes anti-tempest
- Driver de vídeo criptografado
- Variação do Clock
- Diminuir as trilhas desnecessárias dos circuitos de RF
- Blindagem de monitores.

TinFoil Hat Linux



Referências

Faraday Cage – webphysics.davidson.edu/Applets/Poisson/Faraday.html
Electromagnetic Magnetic Eavesdropping Risks of flat-pannel Display - Markus G. Khun Univ. Of Cambridge
Compromising Emanations: eavesdropping risks of computer displays - Markus G. Khun Univ. Of Cambridge
A Concrete That Percolates, Keeping Snow and Spies at Bay
http://www.nytimes.com/2002/03/21/technology/circuits/21NEXT.html
http://cryptome.org/tempest-cpu.htm
http://cryptome.org/tempest-time.htm
http://www.usace.army.mil/inet/usace-docs/eng-pamphlets/ep1110-3-2/toc.htm
http://slashdot.org/science/02/03/21/1838258.shtml
http://www.cotse.com/nix/infowar/tempest/
Macintosh tempest free - http://userwww.sfsu.edu/~hl/c.Tempest.Mac.html
http://www.tempestusa.com/
http://www.cl.cam.ac.uk/~mgk25/
http://tinfoilhat.shmoo.com/

http://www.wiley.com/legacy/compbooks/mcnamara/links.html
Tempest Inc. - http://www.tempest-inc.com/home.htm
http://www.cl.cam.ac.uk/~mgk25/emsec/optical-faq.html
Engineering and Design - Electromagnetic Pulse (EMP) and Tempest Protection for Facilities
Proponent: CEMP-ET
http://www.usace.army.mil/inet/usace-docs/eng-pamphlets/ep1110-3-2/toc.htm

“Segurança é um processo e não um produto.”

-Bruce Schneier
Criador do Blowfish

Contatos

Diego Protta Casati
(KZATY)
kzaty@yahoo.com.br
diego.casati@gmail.com